1. TITLE: ACCEPTABLE USE OF STATE AND PERSONAL ASSETS

2. PURPOSE

State of Colorado information, applications and systems are essential to its success. Authorized Users must use or access the State of Colorado (State) IT resources through authorized and controlled processes and technologies. The Governor's Office of Information Technology (OIT) has an interest and obligation under state statutes to ensure secure, effective, efficient operation and management of these information technology resources. OIT establishes and adopts this Acceptable Use Policy to define the responsibilities of all employees of the Governor's Office to protect State IT resources appropriately.

3. POLICY

All State IT resources, information, and data are the sole property of the State of Colorado and applicable statutes, policies and guidelines govern their use. All Users must use State IT resources in an acceptable manner as defined below in Section 7. All Users must acknowledge reading this policy by signing the document within 30 days of hire date, or 30 days from when this policy goes into effect, and submitting a copy to their HR unit for retention in their personnel files.

OIT has the right to monitor any User's State network, Internet, system or email accounts, and their usage for legitimate business reasons, including monitoring all IT resource performance, employee performance, compliance with this policy, compliance with any applicable laws and industry regulations, and where there is reasonable suspicion of activities that may violate this policy.

Additionally, the State of Colorado has the right to monitor any User's state network, state Internet system, or state email account, whether on a state-issued or personal device.

4. ORGANIZATIONS AFFECTED

The scope of this policy defines the obligations of Users, as defined in Section 6, in using State IT resources owned, managed, supported, maintained or operated by OIT. While this policy contains specific information regarding expected use of State IT resources, employees must also abide by all additional requirements stated in Colorado Cyber Security Policies.

5. REFERENCES

Chief Information Security Officer - C.R.S. §24-37.5-401(1), C.R.S. §24-37.5-403(2)(b)-(c), and C.R.S. §24-37.5-404(2)(b).

6. DEFINITIONS

6.1. Information technology (IT) resource - Computer equipment, communications equipment, storage media, applications, systems, and devices that are: 1) connected to a State of Colorado network; and/or 2) used to process, store, and/or transmit State of Colorado data.

6.2. User - For purposes herein, the term "User" shall include all employees of the Governor's Office, contractors and third-party vendors who have access to State IT resources.

6.3. Information technology (IT) resource owner - The IT or business leader and/or business subject matter expert responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT resource.

6.4. Personally Identifiable Information (PII) – Any information concerning a data subject, which, because of name, number, symbol, mark or other identifier, can be used to identify that data subject.

6.5. Sensitive information – Any information which the loss, misuse, or unauthorized access to or modification of could adversely affect the interest of the state, the conduct of programs, or the privacy to which individuals are entitled.

6.6. Portable device – Defines a smartphone, laptop, tablet (e.g., iPhone, Android, iPad, etc.), or portable drive, that has the ability to access State resources, including its network.

6.7. Personal IT resources – any IT resource that is owned by the User.

6.8. State IT resources – any IT resource that is owned by the State.

7. STANDARDS

7.1. Data Protection

7.1.1. 7.1.1 Users shall obey all data protection requirements, as defined in Cyber Security Policy P-CCSP-011, and will not send or disseminate PII, regulated, or confidential information in an unencrypted form over a State network or the Internet.

7.1.2. 7.1.2 Users shall password protect all IT assets that are used to access State information and that are connected to State IT infrastructure.

7.1.3. 7.1.3 Users may learn, or have access to, sensitive information concerning State and/or agency business, State of Colorado residents, and employee data. It is the responsibility of Users to maintain the confidentiality of all State information. Users must take precautions to protect the unauthorized or careless disclosure of this information.

7.1.4. 7.1.4 No sensitive data shall be downloaded or stored on a personal IT resource, including personal portable devices, computers, external hard drives, CDs/DVDs, or USBs.

7.2. Acceptable Use

7.2.1. Internet

7.2.1.1. The Internet is used to conduct State business. Limited or occasional personal use of the Internet is permitted as outlined in the Personal Use section. Individual job functions will determine the Internet services approved for a User. The fewest privileges consistent with job duties will be assigned.

7.3. Email/Text/Chat/Instant Messaging (IM)

7.3.1. All emails, texts, chat, and instant messages sent to and from State-assigned email, text, chat and instant message accounts are property of the State. Users shall use email to further the goals and objectives of the State of Colorado. The types of activities that are acceptable include:

- Communicating with fellow employees, business partners, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

7.4. Personal Use

7.4.1. The use of State IT resources, specifically email, Internet or telephone, for occasional, incidental personal use is acceptable. However, the following guidelines should be followed:

- Users must still comply with all provisions of this policy and all applicable policies, guidelines and laws.
- Such use must not overly consume scarce State resources (e.g., bandwidth, disk storage space, printing supplies, etc.).
- If a User's usage of a State IT resource is deemed unacceptable or it is impeding their ability to perform their job duties, the employee's supervisor has the right to restrict access, and or initiate corrective action.

7.4.2. Should a User engage State IT resources for personal confidential transactions (such as online banking or credit card usage), the State is not responsible or liable for the confidentiality of any personal data transmitted.

7.5. Remote Access

7.5.1. Employees accessing State information and processes must safeguard their device from loss or theft.

7.5.2. Remote access Users shall only connect to State IT infrastructure through secure encrypted channels that are authorized by agency management.

7.5.3. Remote access Users shall ensure that both State-owned and personally-owned information assets used to connect to State IT infrastructure are password protected and use up-to-date operating system software and security software (i.e., anti-virus, anti-spyware, firewall, and host intrusion prevention) every time a remote connection is initiated.

7.5.4. Employees may access State resources with their own devices, as long as they comply with all State requirements as outlined in the Acceptable Use Policy, they have a signed

and documented agreement to abide by this policy in their personnel file, and the assets have been configured in accordance with State security policies and configuration standards.

7.5.5. Devices that are lost or stolen must be reported to the employee's manager and the Information Security Operations Center (isoc@state.co.us) within 24 hours.

7.5.6. The State reserves the right to remotely wipe any device, including an employee owned device if it was used to access State resources.

7.5.7. Data on devices pertaining to State business, including employee owned devices, are subject to the Colorado Open Records Act (CORA) as it pertains to State business.

7.6. Unacceptable Use of State IT Resources

7.6.1. The use of State IT resources for any commercial purpose or for profit is strictly prohibited.

7.6.2. Users may not change the configurations of any IT resource. Users may be grouped such that their group membership defines specific installation and configuration permissions. Users may not take any unauthorized, deliberate action, which damages, disrupts a State IT resource, alters, or degrades its normal performance, or causes it to malfunction.

7.6.3. Users may not intentionally use State IT resources to access, or attempt to access, any machine, IT resource, network, file or information that they are not authorized to access by virtue of the privileges associated with their user account. This includes information within their Division, the Department, the State, or any external IT resource. Such unauthorized access may constitute a violation of law and be subject to penalty under law, as well as disciplinary action by OIT.

7.6.4. Users may not download or install software on a State IT resource without permission or coordination of the User's Appointing Authority. All unauthorized software will be removed upon discovery. Examples of unauthorized software include but are not limited to:

- Online gaming software
- Games (other than those that come standard with the device)
- Unauthorized shareware or freeware
- Unauthorized hacking or security software
- Software intended for personal use (e.g., Quicken, TurboTax, Greeting Cards, etc.)
- Registry cleaners
- Peer-to-peer software
- Personal firewalls
- Malware, to include but not limited to, Viruses, Trojans, Spyware or Adware

7.6.5. Users' Internet usage must comply with all federal and State of Colorado laws and all State of Colorado policies. Examples of inappropriate use on a state asset, or on a personal device for which the employee is receiving state issued reimbursement (i.e., Bring Your Own Device "BYOD") include the following actions and items that are strictly prohibited, but are not limited to, the following:

- Online gaming
- Visiting online pornography sites
- Sending pornographic text or images
- Participating in online auctions
- Unauthorized copying of State information (or other information intended for official business) to removable media (e.g., CDs, thumb drives, DVDs, etc.) or sending it to an unauthorized address
- Unauthorized postings to blog sites, unauthorized newsgroups, chat rooms, or discussion boards
- Purposefully altering, disabling, or circumventing security features and mechanisms on State IT resources and networks
- Purposefully tampering with or attempting to turn off monitoring software on an IT resource
- Unauthorized attachment of personal computers, laptops, handheld computers, smartphones, modems, etc. to a State IT resource or network
- Illegal file sharing (e.g., software, software keys, passwords, files, music, videos, etc.)
- Sending harassing, threatening, or hate-oriented content
- Creating and or knowingly sending spam or information that is sensitive and confidential to outside parties
- Creating and or knowingly sending malicious code
- Engaging in phishing or other fraudulent activities
- Intercepting data intended for others on the network
- Using spoofing techniques to disguise email addresses or other network activity
- Unauthorized access to any State IT resource
- Using network resources to store personal data or files
- Unauthorized attachment of wireless access points to a State network
- Unauthorized streaming of audio or video files

- Sending or downloading copyrighted material unless authorized by the copyright holder

7.6.6. Internet addresses of sites containing racial, sexual, obscene, harassing, criminal, subversive or other information which violate local, state, federal laws and regulations, or OIT Policies and Procedures may be blocked by OIT.

7.6.7. State IT resources must not be used for purposes of creating, accessing, viewing, retrieving, storing or disseminating any of the following:

- Harassing, threatening, hate-oriented or defamatory materials
- Sexually-oriented, sexually-explicit, obscene or pornographic materials

7.7. Copyright Material

7.7.1. Copyright law subjects the State and its employees to the terms of software license agreements and similar restrictions on other products covered by copyright (e.g., electronic media items such as documents, books, photos, music or videos). State IT resources must be used in accordance with the terms of software license agreements or other copyright restrictions in order to protect the State, its officials and Users from possible legal action. Questions concerning copyright or license issues may be directed to the User's Appointing Authority and/or to their supervisor. It is the responsibility of the User's Appointing Authority to ensure the maintenance and availability of documentation demonstrating software license compliance.

7.8. Right to Monitor

7.8.1. State IT resources and all information and data which are the sole property of (or are controlled by) the State of Colorado and their use is governed by a variety of applicable statutes, policies and guidelines. OIT has the right to monitor any employee's IT resource, network, Internet, e-mail accounts, and their usage, for legitimate business reasons, on either a State owned asset or BYOD device, including monitoring State IT resource performance, employee performance, compliance with this policy, compliance with any applicable laws and industry regulations, and where there is reasonable suspicion of activities that may violate this policy.

7.8.2. By making use of State IT resources, Users consent to allow all information they store on State IT resources to be divulged to State Management, State Human Resources, and/or law enforcement, at the discretion of State Management and State Human Resources.

7.9. Incident Reporting

7.9.1. If an event, such as a seemingly malicious pop-up, virus warning, or other suspicious activity occurs, Users are required to report the incident to the Chief Information Security Officer (CISO), the Information Security Operations Center (isoc@state.co.us), and to their reporting supervisor/manager. Examples of incidents include, but are not limited to:

- Unusual Pop-ups and/or Virus Warnings
- Suspicious callers attempting to obtain unauthorized information such as a User's password or other personnel information
- Suspected attempts (either failed or successful) to gain unauthorized access to an IT resource or its data by unauthorized parties
- The unauthorized use of an IT resource for the processing or storage of data

7.10. Privacy

7.10.1. Users of State IT resources should have no expectation of privacy or confidentiality in their use of a State IT resource. All State records, with minimal exception, are subject to the Colorado Open Records Act, Colorado Revised Statutes Title 24, Article 72. OIT management, technical administrators, and security personnel will periodically monitor the usage of State IT resources to ensure they are operated in a secure, effective, efficient, lawful and ethical manner.

7.10.2. Computer files that are created, entered, stored, or downloaded to a State IT resource, and transmissions sent or received by Users, including those sent or received by email, instant message, voicemail, telephone or over the Internet can be accessed and monitored by authorized personnel at OIT at any time, for any reason without the prior consent of the User. As such, Users should have no expectation of privacy in using a State IT resource.

8. RESPONSIBILITIES

8.1. Supervisors – Responsible for ensuring that his/her subordinates have read, understand, and signed this Acceptable Use Policy within 30 days of hire or when this policy goes into effect and all other security policies as a condition of employment or a condition for granting access.

8.2. Users – Responsible for reading, understanding and adhering to this Acceptable Use Policy. Users are responsible for acknowledging and signing the Acceptable Use Policy within 30 days of hire or when this policy goes into effect.

8.3. System Administrators (SA) –Responsible for reading and understanding all State Cyber Security policies. Additionally, SAs are responsible for managing access and security to the State's IT resources as defined in the State Cyber Security policies.

9. COMPLIANCE

9.1. Misuse of State of Colorado IT resources, as well as other violations of this policy may result in corrective or disciplinary action, up to and including immediate termination of employment. Termination may be warranted, even on the first offense, depending on the seriousness of the misconduct. Discipline is the responsibility of the Appointing Authority, working in conjunction with Human Resources.

9.2. OIT reserves the right to limit privilege of access or terminate the use of its applications and IT resources at any time for any valid technical or policy reason, including for purposes of investigation into possible violations of law or this policy.

9.3. Any violations of law will be reported to appropriate authorities and OIT will cooperate with the authorities in any investigation, providing any information necessary.

10. EXPIRATION

This policy will remain in effect until modified or changed by the Governor's Office of Information Technology.

Signature Page
Governor's Office of Information of Technology
Acceptable Use Policy

As a state employee, contractor or other User of a State IT resource, I acknowledge that I have read and understand the Governor's Office of Information Technology (OIT) Acceptable Use Policy. I further understand and acknowledge that it is my responsibility for obeying all local, state, and federal laws, including those governing copyright and intellectual property, as well as this policy and any applicable State, Department or Division policies.

I agree to abide by these policies and procedures and acknowledge that when an instance of non-compliance is suspected or discovered, proper corrective or disciplinary action may be taken, up to and including termination in accordance with state regulations. Criminal or civil action may be initiated where appropriate. I also understand that when using state IT resources, I have no expectation of privacy and, if required, OIT management may monitor or investigate my usage.

Employee Name (printed)	Working Job Title
Employee Signature	Date
Human Resources Signature	Date